

Ref. ②

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-313979

(P2001-313979A)

(43) 公開日 平成13年11月9日 (2001.11.9)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード* (参考)
H 0 4 Q 7/38		G 0 6 F 13/00	5 1 0 S 5 H 1 8 0
G 0 6 F 13/00	5 1 0	G 0 8 G 1/087	5 K 0 3 3
G 0 8 G 1/087		H 0 4 B 7/26	1 0 9 S 5 K 0 6 7
H 0 4 L 12/28		H 0 4 L 11/00	3 1 0 B

審査請求 未請求 請求項の数10 O L (全 18 頁)

(21) 出願番号 特願2000-128900(P2000-128900)

(22) 出願日 平成12年4月28日 (2000.4.28)

(71) 出願人 000000295

沖電気工業株式会社

東京都港区虎ノ門1丁目7番12号

(72) 発明者 卯木 輝彦

東京都港区虎ノ門1丁目7番12号 沖電気  
工業株式会社内

(74) 代理人 100090620

弁理士 工藤 宜幸

Fターム(参考) 5H180 AA12 JJ02 JJ10

5K033 AA03 BA04 CB01 DA19 DB12

DB14 EA07

5K067 AA21 BB03 BB04 DD17 EE02

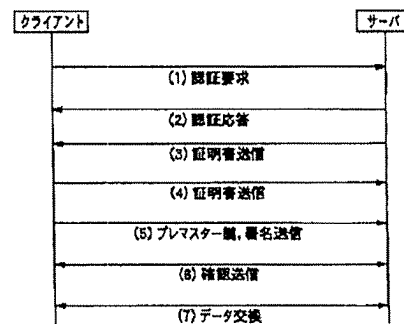
EE10 EE16 EE24 HH11 HH23

## (54) 【発明の名称】 移動端末接続方法

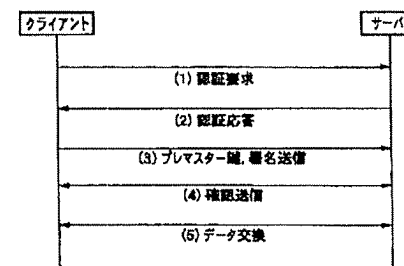
## (57) 【要約】

【課題】 異なる無線通信エリアに移動する度に実行される認証動作が負担となっている。

【解決手段】 クライアントとして機能する移動端末と、通信範囲の限定された複数の無線通信エリアを管理下におき、いずれかの無線通信エリアに入った移動端末と所定の通信サービスを実現するサーバとを備える通信システムにおける移動端末接続方法において、移動端末とサーバは、それぞれ初回の無線接続で交換した固有の認証に関する情報を接続完了後もそのまま保持する機能を搭載し、同一の移動端末及びサーバ間での再度の無線接続時に当該認証に関する情報の無線通信による交換動作を省略する。



(a) 第1実施形態におけるサーバ/クライアント間初期接続シーケンス



(b) 第1実施形態におけるサーバ/クライアント間再接続シーケンス

## 【特許請求の範囲】

【請求項 1】 クライアントとして機能する移動端末と、通信範囲の限定された複数の無線通信エリアを管理下におき、いずれかの無線通信エリアに入った移動端末と所定の通信サービスを実現するサーバとを備える通信システムにおける移動端末接続方法において、上記移動端末とサーバに、それぞれ初回の無線接続で交換した固有の認証に関する情報を接続完了後もそのまま保持する機能を搭載し、同一の移動端末及びサーバ間での再度の無線接続時に当該認証に関する情報の無線通信による交換動作を省略することを特徴とする移動端末接続方法。

【請求項 2】 クライアントとして機能する移動端末と、通信範囲の限定された複数の無線通信エリアを管理下におき、いずれかの無線通信エリアに入った移動端末と所定の通信サービスを実現するサーバとを備える通信システムにおける移動端末接続方法において、上記サーバは、移動端末が保持する当該端末固有の認証に関する情報を接続完了後も保持する手段と、当該端末と上記認証に関する情報を対応付ける手段とを有するものであり、上記移動端末は、起動後、サーバとの最初の無線接続時に上記認証に関する情報を送信し、上記サーバは、上記認証に関する情報を対応付けるための情報と対応させて保持すると共に、上記認証に関する情報を対応付けるための情報を当該移動端末に送信し、上記移動端末は、サーバへの再接続時に、上記認証に関する情報を対応付けるための情報を送信し、上記サーバは、上記認証に関する情報を対応付けるための情報によって、当該移動端末の認証に関する情報を取り出し、当該取り出した移動端末の認証に関する情報を基に移動端末の認証を行うことを特徴とする移動端末接続方法。

【請求項 3】 クライアントとして機能する移動端末と、通信範囲の限定された 1 つ又は複数の無線通信エリアを管理下におき、いずれも自身の管理下にある無線通信エリアに入った移動端末と所定の通信サービスを実現するネットワークを介して接続された複数のサーバとを備える通信システムにおける移動端末接続方法において、上記移動端末が移動した結果、直前まで接続していたとは異なるサーバ間で新たな無線接続が生じた場合、新たに無線接続の対象となったサーバは、当該接続時に移動端末から受信された直前まで接続していたサーバに関する情報に基づいて、該当するサーバに対して交換されていた認証に関する情報の転送を要求し、再度の認証に関する情報の無線通信による交換動作を一部省略することを特徴とする移動端末接続方法。

【請求項 4】 クライアントとして機能する移動端末と、通信範囲の限定された 1 つ又は複数の無線通信エ

リアを管理下におき、いずれも自身の管理下にある無線通信エリアに入った移動端末と所定の通信サービスを実現するネットワークを介して接続された複数のサーバとを備える通信システムにおける移動端末接続方法において、

上記サーバは、移動端末が保持する当該端末固有の認証に関する情報を接続完了後も保持する手段と、当該端末と上記認証に関する情報を対応付ける手段と、現に保持している端末固有の認証に関する情報を他のサーバからの要求に応じ転送する手段とを有するものであり、上記移動端末は、起動後、第 1 のサーバとの最初の無線接続時に自身に固有の認証に関する情報を送信し、上記第 1 のサーバは、上記認証に関する情報を対応付けるための情報と対応させて保持すると共に、上記認証に関する情報を対応付けるための情報と自身の位置情報を当該移動端末に送信し、上記移動端末は、上記第 1 のサーバとネットワークを介して接続された第 2 のサーバへの接続時に、上記認証に関する情報を対応付けるための情報と上記第 1 のサーバの位置情報を送信し、上記第 2 のサーバは、上記認証に関する情報を対応付けるための情報を上記第 1 のサーバに転送することによって当該端末の認証に関する情報の転送を要求し、上記第 1 のサーバは、上記第 2 のサーバの要求する認証に関する情報を対応付けるための情報を基に自身の保持する認証に関する情報を検索し、該当する認証に関する情報が存在する場合、当該情報を第 2 のサーバに転送し、上記第 2 のサーバは、上記第 1 のサーバから転送を受けた認証に関する情報に基づいて新たに接続した移動端末の認証を行うことを特徴とする移動端末接続方法。

【請求項 5】 クライアントとして機能する移動端末と、通信範囲の限定された 1 つ又は複数の無線通信エリアを管理下におき、いずれも自身の管理下にある無線通信エリアに入った移動端末と所定の通信サービスを実現するネットワークを介して接続された複数のサーバとを備える通信システムにおける移動端末接続方法において、上記サーバは、初回の無線接続で交換した移動端末に固有の認証に関する情報を、当該移動端末が次に接続する可能性のある他の全てのサーバに対し予め転送する機能を搭載し、新たに無線接続の対象となったサーバとの認証に関する情報の無線通信による交換動作を一部省略することを特徴とする移動端末接続方法。

【請求項 6】 クライアントとして機能する移動端末と、通信範囲の限定された 1 つ又は複数の無線通信エリアを管理下におき、いずれも自身の管理下にある無線通信エリアに入った移動端末と所定の通信サービスを実現するネットワークを介して接続された複数のサーバとを備える通信システムにおける移動端末接続方法におい

て、

上記サーバは、移動端末が保持する当該端末固有の認証に関する情報を接続完了後も保持する手段と、当該端末と上記認証に関する情報を対応付ける手段と、現に保持している端末固有の認証に関する情報をネットワークを介し接続された他のサーバであって次に当該端末と接続する可能性のある全てのサーバに予め転送する手段とを有するものであり、

上記移動端末は、起動後、第1のサーバとの最初の無線接続時に自身に固有の認証に関する情報を送信し、

上記第1のサーバは、上記認証に関する情報を、当該情報に対応付けるための情報と対応させて保持すると共に、これら情報を自身とネットワークを介し接続された他のサーバであって次に当該移動端末と接続する可能性のある全てのサーバに予め転送し、

上記移動端末は、上記第1のサーバとネットワークを介して接続された第2のサーバへの接続時に、上記認証に関する情報を対応付けるための情報を送信し、

上記第2のサーバは、上記認証に関する情報を対応付けるための情報を基に予め第1のサーバから転送を受けた情報を検索し、該当する認証に関する情報が存在する場合、当該情報に基づいて新たに接続した移動端末の認証を行うことを特徴とする移動端末接続方法。

【請求項7】 クライアントとして機能する移動端末と、通信範囲の限定された1つ又は複数の無線通信エリアを管理下におき、いずれも自身の管理下にある無線通信エリアに入った移動端末と所定の通信サービスを実現するネットワークを介して接続された複数のサーバとを備える通信システムにおける移動端末接続方法において、

上記サーバは、初回の無線接続で交換した移動端末に固有の認証に関する情報を、当該移動端末について事前に設定のあった移動経路上に位置する他の全てのサーバに対し予め転送する機能を搭載し、新たに無線接続の対象となったサーバとの認証に関する情報の無線通信による交換動作を一部省略することを特徴とする移動端末接続方法。

【請求項8】 クライアントとして機能する移動端末と、通信範囲の限定された1つ又は複数の無線通信エリアを管理下におき、いずれも自身の管理下にある無線通信エリアに入った移動端末と所定の通信サービスを実現するネットワークを介して接続された複数のサーバとを備える通信システムにおける移動端末接続方法において、

上記サーバは、移動端末が保持する当該端末固有の認証に関する情報を接続完了後も保持する手段と、当該端末と上記認証に関する情報を対応付ける手段と、現に保持している端末固有の認証に関する情報をネットワークを介し接続された他のサーバであって当該移動端末について事前に設定のあった移動経路上に位置する他の全ての

サーバに予め転送する手段とを有するものであり、

上記移動端末は、起動後、第1のサーバとの最初の無線接続時に自身に固有の認証に関する情報と、事前に設定のあった移動経路に関する情報を送信し、

上記第1のサーバは、上記認証に関する情報を、当該情報に対応付けるための情報とを対応させて保持すると共に、これら情報を自身とネットワークを介し接続された他のサーバであって当該移動端末について事前に設定のあった移動経路上に位置する他の全てのサーバに予め転送し、

上記移動端末は、上記第1のサーバとネットワークを介して接続された第2のサーバへの接続時に、上記認証に関する情報を対応付けるための情報を送信し、

上記第2のサーバは、上記認証に関する情報を対応付けるための情報を基に予め第1のサーバから転送を受けた情報を検索し、該当する認証に関する情報が存在する場合、当該情報に基づいて新たに接続した移動端末の認証を行うことを特徴とする移動端末接続方法。

【請求項9】 クライアントとして機能する移動端末と、通信範囲の限定された1つ又は複数の無線通信エリアを管理下におき、いずれも自身の管理下にある無線通信エリアに入った移動端末と所定の通信サービスを実現するネットワークを介して接続された複数のサーバとを備える通信システムにおける移動端末接続方法において、

上記サーバは、初回の無線接続で交換した移動端末に固有の認証に関する情報を、当該認証に関する情報に対応付ける情報であって有効期限の付いたものと共に、当該移動端末について事前に設定のあった移動経路上に位置する他の全てのサーバに対し予め転送する機能を搭載し、新たに無線接続の対象となったサーバとの認証に関する情報の無線通信による交換動作を一部省略することを特徴とする移動端末接続方法。

【請求項10】 クライアントとして機能する移動端末と、通信範囲の限定された1つ又は複数の無線通信エリアを管理下におき、いずれも自身の管理下にある無線通信エリアに入った移動端末と所定の通信サービスを実現するネットワークを介して接続された複数のサーバとを備える通信システムにおける移動端末接続方法において、

上記サーバは、移動端末が保持する当該端末固有の認証に関する情報を接続完了後も保持する手段と、当該端末と上記認証に関する情報を対応付ける手段と、現に保持している端末固有の認証に関する情報をネットワークを介し接続された他のサーバであって当該移動端末について事前に設定のあった移動経路上に位置する他の全てのサーバに予め転送する手段と、移動端末が移動経路上を移動するのに要する時間を推定する手段とを有するものであり、

上記移動端末は、起動後、第1のサーバとの最初の無線

接続時に自身に固有の認証に関する情報と、事前に設定のあった移動経路に関する情報を送信し、

上記第 1 のサーバは、上記認証に関する情報を、当該情報に対応付けるための情報とを対応させて保持すると共に、これら情報を自身とネットワークを介し接続された他のサーバであって当該移動端末について事前に設定のあった移動経路上に位置するサーバのそれぞれに各サーバを通過するのに要すると推定された有効時間を付して予め転送し、

上記移動端末は、上記第 1 のサーバとネットワークを介して接続された第 2 のサーバへの接続時に、上記認証に関する情報に対応付けるための情報を送信し、

上記第 2 のサーバは、上記認証に関する情報に対応付けるための情報を基に予め第 1 のサーバから転送を受けた情報を検索し、該当する認証に関する情報が存在する場合、当該情報に基づいて新たに接続した移動端末の認証を行うと共に、当該情報をその有効時間の経過後に削除することを特徴とする移動端末接続方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、携帯端末や車載情報機器などの移動可能なクライアントを通信範囲の限定された無線通信により直近のサーバと接続しサービスの提供を可能とするシステムにおいて、クライアントとサーバ間の接続を簡略化する接続方法に関するものである。

【0002】

【従来の技術】現在、携帯端末や車載情報機器などの移動可能なクライアントを通信範囲の限定された無線通信により直近のサーバと接続し、サービスの提供を可能とするシステムとして様々なものが実際に運用されている。例えば、緊急車両直前の青信号を延長するシステム、周辺情報を提供するシステムなどがある。

【0003】このうち、緊急車両直前の青信号を延長するシステムは、緊急車両がなるべく早く目的地に到着できるように、緊急車両前方の信号機を青色にしておくシステムである。このシステムは、無線通信装置、クライアント、サーバなどで構成される。

【0004】無線通信装置は、信号機の直前の道路上に固定的に極小な無線通信エリアを持つように設置される。他方、クライアントは、緊急車両に搭載され、無線通信エリアにあるときのみ無線通信装置を介してサーバと通信可能である。サーバは、無線通信装置及び信号機とネットワークで接続され、信号機の切替えタイミングを制御することができる。無線通信装置は、1つの信号機に1つ以上必要である。サーバは、1つの信号機に1つでも、複数の交差点に1つでも良い。

【0005】クライアントが無線通信エリアに入ると、クライアントとサーバ間で相互認証が行なわれ、クライアントからの要求に応じてサーバが信号機の切替えタイ

ミングを制御する。ここで、サーバは、緊急車両が通過するまで緊急車両前方の信号機を青色にしておく。認証には、暗号鍵の管理が比較的容易な公開鍵による方式がよく使われ、認証プロトコルとしては一般的によく知られたSSLなどが使われることが多い。

【0006】このシステムは、クライアントにGPSなどの位置取得手段が必要なく、サーバ側は信号機周辺の局所的装置だけで実現できるため、導入初期のコストが小さく、サービス提供の地域の拡大も容易である。

10 【0007】他方、周辺情報提供システムは、クライアントの位置に応じて、サーバがクライアントを保持するユーザに有用な情報を提供するシステムである。提供する情報の例として、交通規制や渋滞などの交通情報、空き駐車場情報、休憩所やレストランなどの施設情報などがある。

【0008】このシステムも、前記の青信号延長システムとほぼ同様の構成で実現できる。ただし、無線通信エリアは信号機直前だけに限らない。また、サーバにおける情報の管理は、複数のサーバを情報の種類に応じて適当な階層構造に分け、上位のサーバで行うことも可能である。

【0009】クライアントが、無線通信エリアに入ると、クライアントとサーバ間で相互認証が行なわれ、クライアントからの要求に応じて、サーバは適当な情報を提供する。無線通信エリアを広域にせず、極小な無線通信エリアを特定することで、クライアントの現在位置や進行方向に応じて、きめ細かい情報提供が可能になる。クライアントと対話的に利用することで、駐車場など施設の事前予約なども可能である。

30 【0010】同様の構成で実現できるシステムとして、他にタクシー配車システムやオンデマンドパスシステムなどもある。

【0011】

【発明が解決しようとする課題】しかし、上述のシステム構成の場合には、以下に示すような課題があった。

【0012】1つのクライアントが複数の無線通信エリアを通過しながら、1つのサービスを連続して利用する場合、通信エリアに進入するたびに認証手続きを最初から行う必要があった。

40 【0013】ところが、上記局所的通信を行う無線通信装置にあつては、通常、インフラ整備のコストの問題などから、有線による通信や広域の無線通信に比べ、伝送速度が非常に遅い。

【0014】このため、クライアントが高速移動するシステムでは、無線通信装置によって転送される認証に必要な情報をなるべく小さく抑える必要がある。

【0015】

【課題を解決するための手段】本発明は以上の課題を考慮してなされたもので、かかる課題を解決するため以下の手段を提案する。

【0016】(A)第1の手段としては、初回の接続で交換した認証に関する情報をサーバとクライアントの各々で保存しておき、クライアントが同一サーバを利用する場合には認証手続きを簡略化する方法を提案する。

【0017】(1)すなわち、クライアントとして機能する移動端末と、通信範囲の限定された複数の無線通信エリアを管理下におき、いずれかの無線通信エリアに入った移動端末と所定の通信サービスを実現するサーバを備える通信システムの移動端末接続方法において、移動端末とサーバに、それぞれ初回の無線接続で交換した固有の認証に関する情報を接続完了後もそのまま保持する機能を搭載し、同一の移動端末及びサーバ間での再度の無線接続時に当該認証に関する情報の無線通信による交換動作を省略させる方法を提案する。

【0018】(2)より具体的には、クライアントとして機能する移動端末と、通信範囲の限定された複数の無線通信エリアを管理下におき、いずれかの無線通信エリアに入った移動端末と所定の通信サービスを実現するサーバを備える通信システムの移動端末接続方法において、以下の特徴を備えるものを提案する。

【0019】①サーバは、移動端末が保持する当該端末固有の認証に関する情報を接続完了後も保持する手段と、当該端末と認証に関する情報を対応付ける手段とを有するものである。

【0020】②移動端末は、起動後、サーバとの最初の無線接続時に認証に関する情報を送信する。③サーバは、認証に関する情報を対応付けるための情報と対応させて保持すると共に、認証に関する情報を対応付けるための情報を当該移動端末に送信する。④移動端末は、サーバへの再接続時に、認証に関する情報を対応付けるための情報を送信する。⑤サーバは、認証に関する情報を対応付けるための情報によって、当該移動端末の認証に関する情報を取り出し、当該取り出した移動端末の認証に関する情報を基に移動端末の認証を行う。

【0021】(B)第2の手段としては、クライアントが、複数のサーバを続けて利用する場合に、新たに接続するサーバが直前に接続していたサーバに対して初回の接続で交換した認証に関する情報を要求することで、同一セキュリティドメインのサーバの再接続における認証手続きを簡略化する方法を提案する。

【0022】(1)すなわち、クライアントとして機能する移動端末と、通信範囲の限定された1つ又は複数の無線通信エリアを管理下におき、いずれも自身の管理下にある無線通信エリアに入った移動端末と所定の通信サービスを実現するネットワークを介して接続された複数のサーバとを備える通信システムにおける移動端末接続方法において、移動端末が移動した結果、直前まで接続していたのとは異なるサーバ間で新たな無線接続が生じた場合、新たに無線接続の対象となったサーバは、当該接続時に移動端末から受信された直前まで接続していた

サーバに関する情報に基づいて、該当するサーバに対して交換されていた認証に関する情報の転送を要求し、再度の認証に関する情報の無線通信による交換動作を一部省略させる方法を提案する。

【0023】(2)より具体的には、クライアントとして機能する移動端末と、通信範囲の限定された1つ又は複数の無線通信エリアを管理下におき、いずれも自身の管理下にある無線通信エリアに入った移動端末と所定の通信サービスを実現するネットワークを介して接続された複数のサーバとを備える通信システムにおける移動端末接続方法において、以下の特徴を備えるものを提案する。

【0024】①サーバは、移動端末が保持する当該端末固有の認証に関する情報を接続完了後も保持する手段と、当該端末と認証に関する情報を対応付ける手段と、現に保持している端末固有の認証に関する情報を他のサーバからの要求に応じ転送する手段とを有するものである。

【0025】②移動端末は、起動後、第1のサーバとの最初の無線接続時に自身に固有の認証に関する情報を送信する。③第1のサーバは、認証に関する情報を対応付けるための情報と対応させて保持すると共に、認証に関する情報を対応付けるための情報と自身の位置情報を当該移動端末に送信する。④移動端末は、第1のサーバとネットワークを介して接続された第2のサーバへの接続時に、認証に関する情報を対応付けるための情報と第1のサーバの位置情報を送信する。⑤第2のサーバは、認証に関する情報を対応付けるための情報を第1のサーバに転送することによって当該端末の認証に関する情報の転送を要求する。⑥第1のサーバは、第2のサーバの要求する認証に関する情報を対応付けるための情報を基に自身の保持する認証に関する情報を検索し、該当する認証に関する情報が存在する場合、当該情報を第2のサーバに転送する。⑦第2のサーバは、第1のサーバから転送を受けたの認証に関する情報に基づいて新たに接続した移動端末の認証を行う。

【0026】(C)第3の手段としては、クライアントが、複数のサーバを続けて利用する場合に、クライアントが次に接続する可能性のあるすべてのサーバに、事前に認証に関する情報を転送しておくことで、同一セキュリティドメインのサーバの再接続における認証手続きを簡略化する方法を提案する。

【0027】(1)すなわち、クライアントとして機能する移動端末と、通信範囲の限定された1つ又は複数の無線通信エリアを管理下におき、いずれも自身の管理下にある無線通信エリアに入った移動端末と所定の通信サービスを実現するネットワークを介して接続された複数のサーバとを備える通信システムにおける移動端末接続方法において、サーバは、初回の無線接続で交換した移動端末に固有の認証に関する情報を、当該移動端末が次

に接続する可能性のある他の全てのサーバに対し予め転送する機能を搭載し、新たに無線接続の対象となったサーバとの認証に関する情報の無線通信による交換動作を一部省略させる方法を提案する。

【0028】(2)より具体的には、クライアントとして機能する移動端末と、通信範囲の限定された1つ又は複数の無線通信エリアを管理下におき、いずれも自身の管理下にある無線通信エリアに入った移動端末と所定の通信サービスを実現するネットワークを介して接続された複数のサーバとを備える通信システムにおける移動端末接続方法において、以下の特徴を備えるものを提案する。

【0029】①サーバは、移動端末が保持する当該端末固有の認証に関する情報を接続完了後も保持する手段と、当該端末と認証に関する情報を対応付ける手段と、現に保持している端末固有の認証に関する情報をネットワークを介し接続された他のサーバであって次に当該端末と接続する可能性のある全てのサーバに予め転送する手段とを有するものである。

【0030】②移動端末は、起動後、第1のサーバとの最初の無線接続時に自身に固有の認証に関する情報を送信する。③第1のサーバは、認証に関する情報を、当該情報に対応付けるための情報と対応させて保持すると共に、これら情報を自身とネットワークを介し接続された他のサーバであって次に当該移動端末と接続する可能性のある全てのサーバに予め転送する。④移動端末は、第1のサーバとネットワークを介して接続された第2のサーバへの接続時に、認証に関する情報を対応付けるための情報を送信する。⑤第2のサーバは、認証に関する情報を対応付けるための情報を基に予め第1のサーバから転送を受けた情報を検索し、該当する認証に関する情報が存在する場合、当該情報に基づいて新たに接続した移動端末の認証を行う。

【0031】(D)第4の手段としては、クライアントが、事前に計画された経路にそって複数のサーバを利用する場合に、クライアントの移動経路上のすべてのサーバに、事前に認証に関する情報を転送しておくことで、同一セキュリティドメインのサーバの再接続における認証手続きを簡略化する方法を提案する。

【0032】(1)すなわち、クライアントとして機能する移動端末と、通信範囲の限定された1つ又は複数の無線通信エリアを管理下におき、いずれも自身の管理下にある無線通信エリアに入った移動端末と所定の通信サービスを実現するネットワークを介して接続された複数のサーバとを備える通信システムにおける移動端末接続方法において、サーバは、初回の無線接続で交換した移動端末に固有の認証に関する情報を、当該移動端末について事前に設定のあった移動経路上に位置する他の全てのサーバに対し予め転送する機能を搭載し、新たに無線接続の対象となったサーバとの認証に関する情報の無線

通信による交換動作を一部省略させる方法を提案する。

【0033】(2)より具体的には、クライアントとして機能する移動端末と、通信範囲の限定された1つ又は複数の無線通信エリアを管理下におき、いずれも自身の管理下にある無線通信エリアに入った移動端末と所定の通信サービスを実現するネットワークを介して接続された複数のサーバとを備える通信システムにおける移動端末接続方法において、以下の特徴を備えるものを提案する。

【0034】①サーバは、移動端末が保持する当該端末固有の認証に関する情報を接続完了後も保持する手段と、当該端末と認証に関する情報を対応付ける手段と、現に保持している端末固有の認証に関する情報をネットワークを介し接続された他のサーバであって当該移動端末について事前に設定のあった移動経路上に位置する他の全てのサーバに予め転送する手段とを有するものである。

【0035】②移動端末は、起動後、第1のサーバとの最初の無線接続時に自身に固有の認証に関する情報と、事前に設定のあった移動経路に関する情報を送信する。③第1のサーバは、認証に関する情報を、当該情報に対応付けるための情報とを対応させて保持すると共に、これら情報を自身とネットワークを介し接続された他のサーバであって当該移動端末について事前に設定のあった移動経路上に位置する他の全てのサーバに予め転送する。④移動端末は、第1のサーバとネットワークを介して接続された第2のサーバへの接続時に、認証に関する情報を対応付けるための情報を送信する。⑤第2のサーバは、認証に関する情報を対応付けるための情報を基に予め第1のサーバから転送を受けた情報を検索し、該当する認証に関する情報が存在する場合、当該情報に基づいて新たに接続した移動端末の認証を行う。

【0036】(E)第5の手段としては、クライアントが、事前に計画された経路にそって複数のサーバを利用する場合に、クライアントの次の移動経路上のサーバに、事前に認証に関する情報を転送しておくことで、同一セキュリティドメインのサーバの再接続における認証手続きを簡略化し、さらに、認証に関する情報の有効期限を設けることで、資源の有効利用を可能にする方法を提案する。

【0037】(1)すなわち、クライアントとして機能する移動端末と、通信範囲の限定された1つ又は複数の無線通信エリアを管理下におき、いずれも自身の管理下にある無線通信エリアに入った移動端末と所定の通信サービスを実現するネットワークを介して接続された複数のサーバとを備える通信システムにおける移動端末接続方法において、サーバは、初回の無線接続で交換した移動端末に固有の認証に関する情報を、当該認証に関する情報に対応付ける情報であって有効期限の付いたものと共に、当該移動端末について事前に設定のあった移動経

路上に位置する他の全てのサーバに対し予め転送する機能を搭載し、新たに無線接続の対象となったサーバとの認証に関する情報の無線通信による交換動作を一部省略させる方法を提案する。

【0038】(2)より具体的には、クライアントとして機能する移動端末と、通信範囲の限定された1つ又は複数の無線通信エリアを管理下におき、いずれも自身の管理下にある無線通信エリアに入った移動端末と所定の通信サービスを実現するネットワークを介して接続された複数のサーバとを備える通信システムにおける移動端末接続方法において、以下の特徴を備えるものを提案する。

【0039】①サーバは、移動端末が保持する当該端末固有の認証に関する情報を接続完了後も保持する手段と、当該端末と認証に関する情報を対応付ける手段と、現に保持している端末固有の認証に関する情報をネットワークを介し接続された他のサーバであって当該移動端末について事前に設定のあった移動経路上に位置する他の全てのサーバに予め転送する手段と、移動端末が移動経路上を移動するのに要する時間を推定する手段とを有するものである。

【0040】②移動端末は、起動後、第1のサーバとの最初の無線接続時に自身に固有の認証に関する情報と、事前に設定のあった移動経路に関する情報を送信する。

③第1のサーバは、認証に関する情報を、当該情報に対応付けるための情報とを対応させて保持すると共に、これら情報を自身とネットワークを介し接続された他のサーバであって当該移動端末について事前に設定のあった移動経路上に位置するサーバのそれぞれに各サーバを通しての要すると推定された有効時間を付して予め転送する。④移動端末は、第1のサーバとネットワークを介して接続された第2のサーバへの接続時に、認証に関する情報を対応付けるための情報を送信する。⑤第2のサーバは、認証に関する情報を対応付けるための情報を基に予め第1のサーバから転送を受けた情報を検索し、該当する認証に関する情報が存在する場合、当該情報に基づいて新たに接続した移動端末の認証を行うと共に、当該情報をその有効時間の経過後に削除する。

【0041】

【発明の実施の形態】(A)第1の実施形態

ここでは、上述の第1の手段に対応する実施形態を説明する。

【0042】(A-1)システム構成

図2に、本実施形態に係る移動端末接続方法を適用するシステム構成を示す。図中、1はサーバ、2A~2Cは無線通信装置、3はクライアントである。説明を容易にするため、サーバとクライアントは各々1つだけ図示している。

【0043】ここで、サーバ1は、ワークステーションなどの電子計算機に実装されるものであり、複数の無線

通信装置2A~2Cとネットワークを介して接続される。一般にネットワークは有線となるが、無線を排除するものではない。

【0044】無線通信装置2A~2Cは、各々固定された通信エリアを持ち、お互いの無線通信エリアは交わらない。

【0045】クライアント3は、携帯端末など移動可能な電子計算機で実現されるものとし、無線通信装置2A~2Cを介してサーバ1と通信できる機能を含んでいる。

【0046】図3に、サーバ1の機能構成を示す。11は認証部、12は証明書格納部、13は一時的ID発行部、14はサービス実行部、15は通信部である。図4に、クライアント3の機能構成を示す。21は認証部、22は証明書格納部、23は一時的ID格納部、24はサービス実行部、25は無線通信部である。

【0047】ここで、証明書格納部12及び22はRAM等の記憶装置で実現される。一時的ID格納部23も同様である。なお、認証部11及び21、一時的ID発行部13、サービス実行部14及び24の各機能についてはソフトウェア処理又はハードウェア処理のいずれかで実現される。

【0048】(A-2)接続動作

図1に、第1の実施形態で実行される接続動作例を示す。なお、図1(a)は、クライアント3が起動後初めて無線通信エリアに入った場合又は異なるサーバの管理する無線通信エリアに入った場合に実行される初期接続シーケンスを表している。また、図1(b)は、一度認証手続きを済ませたクライアント3が前回と同じサーバが管理する無線通信エリアに再び侵入した場合に実行される再接続シーケンスを表している。

【0049】まず、図1(a)に示す初期接続シーケンスを説明する。このシーケンスでは、初めにクライアント3がサーバに対して認証要求メッセージを送信し

(1)、サーバ1が認証応答メッセージにより応答する(2)。このやりとりにより、暗号アルゴリズムやデータ圧縮方法の交渉が行なわれる。

【0050】サーバ1からの認証応答では、一時的ID発行部13が生成した一時的IDが添付される。一時的IDは、その時点でシステムに存在するクライアントを一意に特定するための識別子である。

【0051】次に、サーバ1はサーバの公開鍵を含む証明書をクライアントに送り(3)、クライアント3はクライアントの公開鍵を含む証明書をサーバに送る

(4)。クライアント3は、一時的IDを一時的ID格納部23に、サーバの証明書を証明書格納部22に保存しておく。サーバ1は、クライアントの証明書を、発行した一時的IDと対応させ、証明書格納部12に保存しておく。

【0052】次に、クライアント3は、プレマスター鍵

をサーバの公開鍵で暗号化し、クライアントの署名をつけて、サーバに送る(5)。

【0053】サーバ1は、メッセージをサーバの秘密鍵で復号化することによりプレマスター鍵をとりだし、クライアントの公開鍵によりクライアントの署名を確認する。クライアント3及びサーバ1ともに、プレマスター鍵により実際の通信に使われるマスター鍵を生成する。

【0054】次に、クライアント3とサーバ1の両方が、通信の準備ができたことを確認するメッセージを送信し(6)、サービスに関するデータ交換を開始する(7)。サービスに関するデータ交換は、マスター鍵により対称暗号方式による暗号化を行う。

【0055】続いて、図1(b)に示す再接続シーケンスを説明する。このシーケンスでは、初めにクライアント3がサーバに対して、認証要求メッセージを送信し(1)、サーバ1が認証応答メッセージにより応答する(2)。クライアント3からの認証要求では、初期接続時にサーバにより付与されクライアントの一時的ID格納部23に保管されていた一時的IDが添付される。

【0056】サーバ1は、送られてきた一時的IDにより、証明書格納部12から対応するクライアントの証明書を取り出す。これにより、初期認証手順と比べて、証明書の交換手順が省略される。以下、初期認証手順と同様である。

【0057】上記の手順は、システムが採用する認証方式により若干異なる場合があるが、いずれの方式においても、一度交換した証明書をサーバとクライアントが保存しておくという点で、証明書交換のためのメッセージ交換が省略できる。

【0058】(A-3)第1の実施形態の効果

以上のように第1の実施形態によれば、サーバとクライアントのそれぞれにおいて、クライアントとサーバが初回の接続時に交換した認証に関する情報を保存しておくため、クライアントが同一サーバを再度利用する場合には証明書の転送を不要にできる。このため、再接続時におけるサーバとクライアントの間の通信量の削減を実現できる。

【0059】(B)第2の実施形態

ここでは、上述の第2の手段に対応する実施形態を説明する。

【0060】(B-1)システム構成

図5に、本実施形態に係る移動端末接続方法を適用するシステム構成を示す。図中、1A~1Cはサーバ、2A~2Cは無線通信装置、3はクライアントである。説明を容易にするため、サーバは3つだけ、クライアントは1つだけ図示している。

【0061】この実施形態でも、サーバ1A~1Cは、ワークステーションなどの電子計算機に実装されるものを用いる。ただし、サーバ1A~1Cは、それぞれ特定の無線通信装置及び他のサーバとネットワークを介して

接続されている。因に、サーバ1Aは無線通信装置2Aと、サーバ1Bは無線通信装置2Bと、サーバ1Cは無線通信装置2Cと接続される。

【0062】無線通信装置2A~2Cは、各々固定された通信エリアを持ち、お互いの無線通信エリアは交わらない。

【0063】クライアント3は、携帯端末など移動可能な計算機で実現されるものとし、無線通信装置2A~2Cを介してサーバ1A~1Cと通信できる機能を含んでいる。

【0064】図6に、サーバ1A~1Cの機能構成を示す。11は認証部、12は証明書格納部、13は一時的ID発行部、14はサービス実行部、15は通信部、16は証明書転送部である。この構成は、証明書転送部16が新たに追加されている点を除いて第1の実施形態に係るサーバと同じ構成である。

【0065】ここで、証明書転送部16は、ネットワークを介して接続されている他のサーバから証明書の要求があった場合に、証明格納部12から該当する証明書を読み出して通信部15に転送する機能を実現するために設けられている。

【0066】図7に、クライアント3の機能構成を示す。21は認証部、22は証明書格納部、23は一時的ID格納部、24はサービス実行部、25は無線通信部、26は直前サーバ位置情報格納部である。この構成は、直前サーバ位置情報格納部26が新たに追加されている点を除いて第1の実施形態に係るクライアントと同じ構成である。

【0067】ここで、直前サーバ位置情報格納部26は、クライアントによる証明書の送信動作を可能な限り削減できるようにするために設けられているもので、直前に接続したサーバの位置情報(必ずしも1つ前の情報に限らず、2つ前の情報でも良い、1つ前と2つ前の2つの情報でも良い。)を格納する。一般に、当該格納部はRAM等の記憶装置で実現される。

【0068】(B-2)接続動作

図8に、第2の実施形態で実行される接続動作の概要を示す。なお、図8(a)は、クライアント3が起動後初めて無線通信エリアに入った場合又は前回接続した無線通信エリアとは接続関係のない他のネットワークの無線通信エリアに入った場合に実行される初期接続シーケンスを表している。また、図8(b)は、一度認証手続きを済ませたクライアント3が前回接続した無線通信エリアと接続関係にあるネットワーク上の他の無線通信エリアに再び侵入した場合に実行される再接続シーケンスを表している。

【0069】以下の説明では、クライアント3が最初に接続するサーバをサーバ1B、次に接続するサーバをサーバ1Aとする。

【0070】まず、図8(a)に示す初期接続シーケ



スを説明する。このシーケンスでは、初めにクライアント 3 がサーバ 1 B に対して認証要求メッセージを送信し (1)、サーバ 1 B が認証応答メッセージにより応答する (2)。このやりとりにより、暗号アルゴリズムやデータ圧縮方法の交渉が行なわれる。

【0071】サーバ 1 B からの認証応答では、一時的 ID 発行部 13 が生成した一時的 ID とこのサーバ 1 B の位置を特定する位置情報が添付される。ここで、位置情報は不図示の記憶装置に格納されていても良いし、一時的 ID 発行部 13 内に格納されていても良い。なお、一時的 ID は、その時点でシステムに存在するクライアントを一意に特定するための識別子である。

【0072】次に、サーバ 1 B はサーバ 1 B の公開鍵を含む証明書をクライアント 3 に送り (3)、クライアント 3 はクライアント 3 の公開鍵を含む証明書をサーバ 1 B に送る (4)。クライアント 3 は、一時的 ID を一時的 ID 格納部 23 に、サーバ 1 B の証明書を証明書格納部 22 に、サーバ 1 B の位置情報を直前サーバ位置情報格納部 26 に保存しておく。サーバ 1 B は、クライアントの証明書を、発行した一時的 ID と対応させ、証明書格納部 12 に保存しておく。

【0073】次に、クライアント 3 は、プレマスター鍵をサーバの公開鍵で暗号化し、クライアントの署名をつけて、サーバに送る (5)。

【0074】サーバ 1 B は、メッセージをサーバ 1 B の秘密鍵で復号化することによりプレマスター鍵をとりだし、クライアントの公開鍵によりクライアントの署名を確認する。クライアント 3 及びサーバ 1 B とともに、プレマスター鍵により実際の通信に使われるマスター鍵を生成する。

【0075】次に、クライアント 3 とサーバ 1 B の両方が、通信の準備ができたことを確認するメッセージを送信し (6)、サービスに関するデータ交換を開始する (7)。サービスに関するデータ交換は、マスター鍵により対称暗号方式による暗号化を行う。

【0076】続いて、図 8 (b) に示す再接続シーケンスを説明する。このシーケンスでは、初めにサーバ 1 A がこの無線通信エリアを分担しているものとする。すなわち、クライアント 3 は前回の接続時から移動しており、サーバ 1 B の管理する無線通信エリアからサーバ 1 A の管理する無線通信エリアに既に移動しているものとする。

【0077】従って、初めにクライアント 3 はサーバ 1 A に対して、認証要求メッセージを送信し (1)、サーバ 1 A が認証応答メッセージにより応答する (2)。クライアント 3 からの認証要求では、初期接続時にサーバ 1 B により付与されクライアントの一時的 ID 格納部 23 に保管されていた一時的 ID と直前サーバ位置情報格納部 26 に保存されていたサーバ 1 B の位置情報が添付される。

【0078】サーバ 1 は、送られてきた位置情報からサーバ 1 B を特定し、ネットワークを介して接続されたサーバ 1 B に対してクライアント 3 の一時的 ID を送り、当該クライアントの証明書を要求する (3)。

【0079】サーバ 1 B は、送られてきた一時的 ID により、証明書格納部 12 から対応するクライアントの証明書を取り出し、サーバ 1 A に返送する (4)。

【0080】これにより、初期認証手順と比べて、クライアント証明書の交換手順が省略される。以下、初期認証手順と同様である。

【0081】上記の手順は、システムが採用する認証方式により若干異なる場合があるが、いずれの方式においても、一度交換した証明書をサーバが保存しておくという点で、証明書交換のためのメッセージ交換が省略できる。

【0082】(B-3) 第 2 の実施形態の効果  
以上のように第 2 の実施形態によれば、クライアントと最初に接続したサーバが、クライアントの認証に関する情報 (証明書) を保存しておくため、クライアントがネットワークを介して接続された複数のサーバを利用する場合にも、次に接続するサーバとクライアントとの間でクライアントの証明書の転送を不要にできる。このため、複数のサーバを順に利用する場合に、次に接続するサーバとクライアントの間の通信量を削減することができる。

【0083】(C) 第 3 の実施形態

(C-1) システム構成

図 9 に、本実施形態に係る移動端末接続方法を適用するシステム構成を示す。図中、1 A ~ 1 C はサーバ、2 A ~ 2 C は無線通信装置、3 はクライアントである。説明を容易にするため、サーバは 3 つだけ、クライアントは 1 つだけ図示している。

【0084】この実施形態でも、サーバ 1 A ~ 1 C は、ワークステーションなどの電子計算機に実装されるものを用いる。ただし、サーバ 1 A ~ 1 C は、それぞれ特定の無線通信装置及び他のサーバとネットワークを介して接続されている。因に、サーバ 1 A は無線通信装置 2 A と、サーバ 1 B は無線通信装置 2 B と、サーバ 1 C は無線通信装置 2 C と接続される。

【0085】無線通信装置 2 A ~ 2 C は、各々固定された通信エリアを持ち、お互いの無線通信エリアは交わらない。

【0086】クライアント 3 は、携帯端末など移動可能な計算機で実現されるものとし、無線通信装置 2 A ~ 2 C を介してサーバ 1 A ~ 1 C と通信できる機能を含んでいる。

【0087】図 10 に、サーバ 1 A ~ 1 C の機能構成を示す。11 は認証部、12 は証明書格納部、13 は一時的 ID 発行部、14 はサービス実行部、15 は通信部、16 は証明書転送部、17 は隣接サーバ情報格納部であ

る。この構成は、隣接サーバ情報格納部 17 が新たに追加されている点を除いて第 2 の実施形態に係るサーバと同じ構成である。

【0088】ここで、隣接サーバ情報格納部 17 は、当該サーバが当該サーバ周辺の他のサーバと通信するための情報を格納するために設けられている。

【0089】図 11 に、クライアント 3 の機能構成を示す。21 は認証部、22 は証明書格納部、23 は一時的 ID 格納部、24 はサービス実行部、25 は無線通信部である。この構成は、第 1 の実施形態に係るクライアントと同じ構成である。

#### 【0090】(C-2) 接続動作

図 12 に、第 3 の実施形態で実行される接続動作の概要を示す。なお、図 12 (a) は、クライアント 3 が起動後初めて無線通信エリアに入った場合又は前回接続した無線通信エリアとは接続関係のない他のネットワークの無線通信エリアに入った場合に実行される初期接続シーケンスを表している。また、図 12 (b) は、一度認証手続きを済ませたクライアント 3 が前回接続した無線通信エリアと接続関係にあるネットワーク上の他の無線通信エリアに再び侵入した場合に実行される再接続シーケンスを表している。

【0091】以下の説明では、クライアント 3 が最初に接続するサーバをサーバ 1 B、次に接続するサーバをサーバ 1 A とする。また、サーバ 1 B の管理する無線通信エリアの周辺には、サーバ 1 A とサーバ 1 C が管理する無線通信エリアがあるものとする。

【0092】まず、図 12 (a) に示す初期接続シーケンスを説明する。このシーケンスでは、初めにクライアント 3 がサーバ 1 B に対して認証要求メッセージを送信し (1)、サーバ 1 B が認証応答メッセージにより応答する (2)。このやりとりにより、暗号アルゴリズムやデータ圧縮方法の交渉が行なわれる。

【0093】サーバ 1 B からの認証応答では、一時的 ID 発行部 13 が生成した一時的 ID が添付される。一時的 ID は、その時点でシステムに存在するクライアントを一意に特定するための識別子である。

【0094】次に、サーバ 1 B はサーバ 1 B の公開鍵を含む証明書をクライアント 3 に送り (3)、クライアント 3 はクライアント 3 の公開鍵を含む証明書をサーバ 1 B に送る (4)。クライアント 3 は、一時的 ID を一時的 ID 格納部 23 に、サーバ 1 B の証明書を証明書格納部 22 に保存しておく。サーバ 1 B は、クライアントの証明書を、発行した一時的 ID と対応させ、証明書格納部 12 に保存しておく。

【0095】次に、クライアント 3 は、プレマスター鍵をサーバの公開鍵で暗号化し、クライアントの署名をつけて、サーバに送る (5)。

【0096】サーバ 1 B は、メッセージをサーバ 1 B の秘密鍵で復号化することによりプレマスター鍵をとりだ

し、クライアントの公開鍵によりクライアントの署名を確認する。クライアント 3 及びサーバ 1 B とともに、プレマスター鍵により実際の通信に使われるマスター鍵を生成する。

【0097】次に、クライアント 3 とサーバ 1 B の両方が、通信の準備ができたことを確認するメッセージを送信し (6)、サービスに関するデータ交換を開始する

(7)。サービスに関するデータ交換は、マスター鍵により対称暗号方式による暗号化を行う。

【0098】サービスに関するデータ交換が終了したとき又はクライアント 3 がサーバ 1 B の管理する無線通信エリアから外に出たとき、サーバ 1 B は、隣接サーバ情報格納部 17 に格納されていたサーバ情報に基づき、サーバ 1 A 及びサーバ 1 C に対して、当該クライアントの証明書及び一時的 ID を転送する。サーバ 1 A 及びサーバ 1 C は、受けとった証明書を一時的 ID と対応させ、証明書格納部 12 に保存する。

【0099】続いて、図 12 (b) に示す再接続シーケンスを説明する。このシーケンスでは、初めにサーバ 1 A がこの無線通信エリアを分担しているものとする。すなわち、クライアント 3 は前回の接続時から移動しており、サーバ 1 B の管理する無線通信エリアからサーバ 1 A の管理する無線通信エリアに既に移動しているものとする。

【0100】従って、初めにクライアント 3 はサーバ 1 A に対して、認証要求メッセージを送信し (1)、サーバ 1 A が認証応答メッセージにより応答する (2)。クライアント 3 からの認証要求では、初期接続時にサーバ 1 B により付与されクライアントの一時的 ID 格納部 23 に保管されていた一時的 ID が添付される。サーバ 1 A は、証明書格納部 12 を探索し、一時的 ID に対応する証明書が見つかった場合、サーバの証明書を送信する (3)。以下、クライアントからの証明書の転送が省略され、それ以降は初期接続手順と同様である。

【0101】上記の手順は、システムが採用する認証方式により若干異なる場合があるが、いずれの方式においても、一度交換した証明書をサーバが保存しておくという点で、証明書交換のためのメッセージ交換が省略できる。

#### 【0102】(C-3) 第 3 の実施形態の効果

以上のように第 3 の実施形態によれば、クライアントと最初に接続したサーバが、クライアントの認証に関する情報 (証明書) を事前に他の周辺サーバに転送しておくため、クライアントが複数のサーバを利用する場合にも、次に接続するサーバとクライアントとの間でクライアントの証明書の転送を不要にできる。このため、複数のサーバを順に利用する場合に、次に接続するサーバとクライアントの間の通信量を削減することができる。しかも、他のサーバへの情報 (証明書) 転送は、クライアントが他のサーバに接続する前に行なわれるので、再接

続時の時間遅延も少なく済む。

#### 【0103】(D)第4の実施形態

##### (D-1)システム構成

図13に、本実施形態に係る移動端末接続方法を適用するシステム構成を示す。図中、1A~1Dはサーバ、2A~2Dは無線通信装置、3はクライアントである。説明を容易にするため、サーバは4つだけ、クライアントは1つだけ図示している。

【0104】この実施形態でも、サーバ1A~1Dは、ワークステーションなどの電子計算機に実装されるものをいう。ただし、サーバ1A~1Dは、それぞれ特定の無線通信装置及び他のサーバとネットワークを介して接続されている。因に、サーバ1Aは無線通信装置2Aと、サーバ1Bは無線通信装置2Bと、サーバ1Cは無線通信装置2Cと、サーバ1Dは無線通信装置2Dと接続される。

【0105】無線通信装置2A~2Dは、各々固定された通信エリアを持ち、お互いの無線通信エリアは交わらない。

【0106】クライアント3は、携帯端末など移動可能な計算機で実現されるものとし、無線通信装置2A~2Dを介してサーバ1A~1Dと通信できる機能を含んでいる。

【0107】図14に、サーバ1A~1Dの機能構成を示す。11は認証部、12は証明書格納部、13は一時的ID発行部、14はサービス実行部、15は通信部、16は証明書転送部、18は経路上サーバ探索部である。この構成は、経路上サーバ探索部18が新たに追加されている点を除いて第2の実施形態に係るサーバと同じ構成である。

【0108】経路上サーバ探索部18は、クライアントから送られてきたクライアントの移動経路情報に基づき、その経路上に存在する他のサーバを検索する手段である。

【0109】図15に、クライアント3の機能構成を示す。21は認証部、22は証明書格納部、23は一時的ID格納部、24はサービス実行部、25は無線通信部、27は移動経路入力部である。この構成は、直前サーバ位置情報格納部26を移動経路入力部27で置き換えた点を除いて第2の実施形態に係るクライアントと同じ構成である。

【0110】ここで、移動経路入力部27は、クライアント3の利用者が移動経路を入力する手段である。もっとも、この移動経路入力部27は、一般的なナビゲーションシステムのように、ユーザは目的地を入力するだけであり、クライアント内で探索される推奨経路の情報を移動経路の入力としても良い。

##### 【0111】(D-2)接続動作

図16に、第4の実施形態で実行される接続動作の概要を示す。なお、図16(a)は、クライアント3が起動

後初めて無線通信エリアに入った場合又は前回接続した無線通信エリアとは接続関係のない他のネットワークの無線通信エリアに入った場合に実行される初期接続シーケンスを表している。また、図16(b)は、一度認証手続きを済ませたクライアント3が前回接続した無線通信エリアと接続関係のあるネットワーク上の他の無線通信エリアに再び侵入した場合に実行される再接続シーケンスを表している。

【0112】以下の説明では、クライアント3が最初に接続するサーバをサーバ1B、クライアントの目的地までの予定移動経路途中にあるサーバを接続する順に、サーバ1A、サーバ1Cとする。サーバ1Dが管理する無線通信エリアは、予定移動経路途中にないものとする。

【0113】まず、図16(a)に示す初期接続シーケンスを説明する。このシーケンスでは、初めにクライアント3がサーバ1Bに対して認証要求メッセージを送信し(1)、サーバ1Bが認証応答メッセージにより応答する(2)。このやりとりにより、暗号アルゴリズムやデータ圧縮方法の交渉が行なわれる。

【0114】クライアント3からの認証要求には、クライアントの予定移動経路情報が添付される。予定移動経路情報は、クライアントの利用者が移動経路入力部27を用いて入力したものである。サーバ1Bからの認証応答では、一時的ID発行部13が生成した一時的IDが添付される。一時的IDは、その時点でシステムに存在するクライアントを一意に特定するための識別子である。

【0115】次に、サーバ1Bはサーバ1Bの公開鍵を含む証明書をクライアント3に送り(3)、クライアント3はクライアント3の公開鍵を含む証明書をサーバ1Bに送る(4)。クライアント3は、一時的IDを一時的ID格納部23に、サーバ1Bの証明書を証明書格納部22に保存しておく。サーバ1Bは、クライアントの証明書を、発行した一時的IDと対応させ、証明書格納部12に保存しておく。

【0116】次に、クライアント3は、プレマスター鍵サーバの公開鍵で暗号化し、クライアントの署名をつけて、サーバに送る(5)。

【0117】サーバ1Bは、メッセージをサーバ1Bの秘密鍵で復号化することによりプレマスター鍵をとりだし、クライアントの公開鍵によりクライアントの署名を確認する。クライアント3及びサーバ1Bともに、プレマスター鍵により実際の通信に使われるマスター鍵を生成する。

【0118】次に、クライアント3とサーバ1Bの両方が、対称暗号方式とマスター鍵による通信の準備ができたことを確認するメッセージを送信し(6)、サービスに関するデータ交換を開始する(7)。サービスに関するデータ交換は、マスター鍵により暗号化して行う。

【0119】サービスに関するデータ交換が終了したと

10

20

30

40

50

き又はクライアント 3 がサーバ 1 B の管理する無線通信エリアから外に出たとき、サーバ 1 B は、クライアント 3 からの認証要求に添付された移動経路情報に基づき、経路上サーバ検索部 18 により、クライアント 3 の移動経路上に無線通信エリアをもつすべてのサーバを検索する。上記の例では、サーバ 1 A とサーバ 1 C が出力される。そして、サーバ 1 B は、これらのサーバに対して、当該クライアントの証明書及び一時的 ID を転送する。

【0120】サーバ 1 A 及びサーバ 1 C は、受けとった証明書を一時的 ID と対応させ、証明書格納部 12 に保存する。

【0121】続いて、図 16 (b) に示す再接続シーケンスを説明する。このシーケンスでは、初めにサーバ 1 A がこの無線通信エリアを分担しているものとする。すなわち、クライアント 3 は前回の接続時から移動しており、サーバ 1 B の管理する無線通信エリアからサーバ 1 A の管理する無線通信エリアに既に移動しているものとする。

【0122】従って、初めにクライアント 3 はサーバ 1 A に対して、認証要求メッセージを送信し (1)、サーバ 1 A が認証応答メッセージにより応答する (2)。クライアント 3 からの認証要求では、初期接続時にサーバ 1 B により付与されクライアントの一時的 ID 格納部 23 に保管されていた一時的 ID が添付される。サーバ 1 A は、証明書格納部 12 を探索し、一時的 ID に対応する証明書が見つかった場合、サーバが証明書を送信する (3)。以下、クライアントからの証明書の転送が省略され、それ以降は初期接続手順と同様である。

【0123】上記の手順は、システムが採用する認証方式により若干異なる場合があるが、いずれの方式においても、一度交換した証明書をサーバが保存しておくという点で、証明書交換のためのメッセージ交換が省略できる。

【0124】(D-3) 第 4 の実施形態の効果  
以上のように第 4 の実施形態によれば、クライアントと最初に接続したサーバが、クライアントの認証に関する情報を事前に予定移動経路上のサーバに転送しておくため、クライアントが複数のサーバを利用する場合にも、次に接続するサーバとクライアントとの間でクライアントの証明書の転送を不要にできる。このため、複数のサーバを順に利用する場合に、次に接続するサーバとクライアントの間の通信量を削減することができる。しかも、他のサーバへの情報転送がクライアントが接続する前に行なわれるので、再接続時の時間遅延も少なく済む。また、証明書の転送先となるサーバは予定移動経路上のものだけなので、システム全体の資源に対する無駄も比較的少なくて済む。

【0125】(E) 第 5 の実施形態

(E-1) システム構成

図 17 に、本実施形態に係る移動端末接続方法を適用す

るシステム構成を示す。図中、1 A ~ 1 C はサーバ、2 A ~ 2 C は無線通信装置、3 はクライアントである。説明を容易にするため、サーバは 3 つだけ、クライアントは 1 つだけ図示している。

【0126】この実施形態でも、サーバ 1 A ~ 1 C は、ワークステーションなどの電子計算機に実装されるものを用いる。ただし、サーバ 1 A ~ 1 C は、それぞれ特定の無線通信装置及び他のサーバとネットワークを介して接続されている。因に、サーバ 1 A は無線通信装置 2 A と、サーバ 1 B は無線通信装置 2 B と、サーバ 1 C は無線通信装置 2 C と接続される。

【0127】無線通信装置 2 A ~ 2 C は、各々固定された通信エリアを持ち、お互いの無線通信エリアは交わらない。

【0128】クライアント 3 は、携帯端末など移動可能な計算機で実現されるものとし、無線通信装置 2 A ~ 2 C を介してサーバ 1 A ~ 1 C と通信できる機能を含んでいる。

【0129】図 18 に、サーバ 1 A ~ 1 C の機能構成を示す。11 は認証部、12 は証明書格納部、13 は一時的 ID 発行部、14 はサービス実行部、15 は通信部、16 は証明書転送部、18 は経路上サーバ検索部、19 は移動時間推定部である。この構成は、移動時間推定部 19 が新たに追加されている点を除いて第 4 の実施形態に係るサーバと同じ構成である。

【0130】移動時間推定部 19 は、クライアントの無線通信エリアの通過時間などからクライアントが次のサーバの無線通信エリアを通過するまでのおおよその時間を推定する手段である。ここでは、正確な推定時間を必要とはしていない。例えば、1 時間単位での推定でも良いし、動的な情報を使わなくても良い。勿論、推定単位は一例であって分単位でも良い。

【0131】図 19 に、クライアント 3 の機能構成を示す。21 は認証部、22 は証明書格納部、23 は一時的 ID 格納部、24 はサービス実行部、25 は無線通信部、27 は移動経路入力部である。この構成は、第 4 の実施形態に係るクライアントと同じ構成である。

【0132】(E-2) 接続動作

図 20 に、第 5 の実施形態で実行される接続動作の概要を示す。なお、図 20 (a) は、クライアントが起動後初めて無線通信エリアに入った場合又は前回接続した無線通信エリアとは接続関係にない他のネットワークの無線通信エリアに入った場合に実行される初期接続シーケンスを表している。また、図 20 (b) は、一度認証手続きを済ませたクライアント 3 が前回接続した無線通信エリアと接続関係のあるネットワーク上の他の無線通信エリアに再び侵入した場合に実行される再接続シーケンスを表している。

【0133】以下の説明では、クライアント 3 が最初に接続するサーバをサーバ 1 B、クライアントの目的地ま

での予定移動経路途中にあるサーバを接続する順に、サーバ 1 A、サーバ 1 C とする。

【0134】まず、図 20 (a) に示す初期接続シーケンスを説明する。このシーケンスでは、初めにクライアント 3 がサーバ 1 B に対して認証要求メッセージを送信し (1)、サーバ 1 B が認証応答メッセージにより応答する (2)。このやりとりにより、暗号アルゴリズムやデータ圧縮方法の交渉が行なわれる。

【0135】クライアント 3 からの認証要求には、クライアントの予定移動経路情報が添付される。予定移動経路情報は、クライアントの利用者が移動経路入力部 27 を用いて入力したものである。サーバ 1 B からの認証応答では、一時的 ID 発行部 13 が生成した一時的 ID 及び一時的 ID の有効期限が添付される。

【0136】ここで、一時的 ID は、その時点でシステムに存在するクライアントを一意に特定するための識別子である。これに対し、一時的 ID の有効期限は、移動時間推定部 19 がクライアントの予定移動経路から推定したクライアントが次に接続予定のサーバを十分通過することができる時刻である。

【0137】次に、サーバ 1 B はサーバ 1 B の公開鍵を含む証明書をクライアント 3 に送り (3)、クライアント 3 はクライアント 3 の公開鍵を含む証明書をサーバ 1 B に送る (4)。クライアント 3 は、一時的 ID を一時的 ID 格納部 23 に、サーバ 1 B の証明書を証明書格納部 22 に保存しておく。サーバ 1 B は、クライアントの証明書を、発行した一時的 ID と対応させ、証明書格納部 12 に保存しておく。

【0138】次に、クライアント 3 は、プレマスター鍵をサーバの公開鍵で暗号化し、クライアントの署名をつけて、サーバに送る (5)。

【0139】サーバ 1 B は、メッセージをサーバ 1 B の秘密鍵で復号化することによりプレマスター鍵をとりだし、クライアントの公開鍵によりクライアントの署名を確認する。クライアント 3 及びサーバ 1 B とともに、プレマスター鍵により実際の通信に使われるマスター鍵を生成する。

【0140】次に、クライアント 3 とサーバ 1 B の両方が、通信の準備ができたことを確認するメッセージを送信し (6)、サービスに関するデータ交換を開始する (7)。サービスに関するデータ交換は、対称暗号方式でマスター鍵により暗号化して行う。

【0141】サービスに関するデータ交換が終了したとき又はクライアント 3 がサーバ 1 B の管理する無線通信エリアから外に出たとき、サーバ 1 B は、クライアント 3 からの認証要求に添付された移動経路情報に基づき、経路上サーバ検索部 18 により、クライアント 3 の移動経路上に次に無線通信エリアをもつサーバを検索する。上記の例では、サーバ 1 A が出力される。そして、サーバ 1 B は、サーバ 1 A に対して、当該クライアントの証

明書、一時的 ID 及びクライアントの移動経路情報を転送する。

【0142】このとき、クライアントの移動経路情報は、サーバに関する部分を除くように加工してから送ってもよい。

【0143】続いて、図 20 (b) に示す再接続シーケンスを説明する。このシーケンスでは、初めにサーバ 1 A がこの無線通信エリアを分担しているものとする。すなわち、クライアント 3 は前回の接続時から移動しており、サーバ 1 B の管理する無線通信エリアからサーバ 1 A の管理する無線通信エリアに既に移動しているものとする。

【0144】従って、初めにクライアント 3 はサーバ 1 A に対して、認証要求メッセージを送信し (1)、サーバ 1 A が認証応答メッセージにより応答する (2)。クライアント 3 からの認証要求では、初期接続時にサーバ 1 B により付与されクライアントの一時的 ID 格納部 23 に保管されていた一時的 ID が添付される。サーバ 1 A は、証明書格納部 12 を探索し、一時的 ID に対応する証明書が見つかった場合、サーバが証明書を送信する (3)。以下、クライアントからの証明書の転送が省略され、それ以降は初期接続手順と同様である。

【0145】上記の手順は、システムが採用する認証方式により若干異なる場合があるが、いずれの方式においても、一度交換した証明書をサーバが保存しておくという点で、証明書交換のためのメッセージ交換が省略できる。

【0146】(E-3) 第 5 の実施形態の効果  
以上のように第 5 の実施形態によれば、クライアントと最初に接続したサーバが、クライアントの認証に関する情報を事前に予定移動経路上のサーバに転送しておくため、クライアントが複数のサーバを利用する場合にも、次に接続するサーバとクライアントの間でクライアントの証明書の転送が不要にできる。このため、複数のサーバを順に利用する場合に、次に接続するサーバとクライアントの間の通信量を削減することができる。しかも、認証に関する情報の有効期限を設けたことにより、資源の有効利用を可能にできる。

【0147】

【発明の効果】(A) 上述のように請求項 1 又は請求項 2 に記載の発明によれば、移動端末とサーバに、それぞれ初回の無線接続で交換した固有の認証に関する情報を接続完了後もそのまま保持する機能を搭載し、同一の移動端末及びサーバ間での再度の無線接続時に当該認証に関する情報の無線通信による交換動作を省略できるようにしたことにより、認証に要する通信負担の軽減を実現できる。

【0148】(B) 上述のように請求項 3 又は請求項 4 に記載の発明によれば、移動端末が移動した結果、直前まで接続していたのとは異なるサーバ間で新たな無線接

続が生じた場合、新たに無線接続の対象となったサーバは、当該接続時に移動端末から受信された直前まで接続していたサーバに関する情報に基づいて、該当するサーバに対して交換されていた認証に関する情報の転送を要求し、再度の認証に関する情報の無線通信による交換動作を一部省略できるようにしたことにより、認証に要する通信負担の軽減を実現できる。

【0149】(C) 上述のように請求項5又は請求項6に記載の発明によれば、サーバは、初回の無線接続で交換した移動端末に固有の認証に関する情報を、当該移動

端末が次に接続する可能性のある他の全てのサーバに対し予め転送する機能を搭載し、新たに無線接続の対象となったサーバとの認証に関する情報の無線通信による交換動作を一部省略できるようにしたことにより、認証に要する通信負担の軽減を実現できる。

【0150】(D) 上述のように請求項7又は請求項8に記載の発明によれば、サーバは、初回の無線接続で交換した移動端末に固有の認証に関する情報を、当該移動端末について事前に設定のあった移動経路上に位置する他の全てのサーバに対し予め転送する機能を搭載し、新たに無線接続の対象となったサーバとの認証に関する情報の無線通信による交換動作を一部省略できるようにしたことにより、認証に要する通信負担の軽減を実現できる。

【0151】(E) 上述のように請求項9又は請求項10に記載の発明によれば、サーバは、初回の無線接続で交換した移動端末に固有の認証に関する情報を、当該認証に関する情報に対応付けられる情報であって有効期限の付いたものと共に、当該移動端末について事前に設定のあった移動経路上に位置する他の全てのサーバに対し予め転送する機能を搭載し、新たに無線接続の対象となったサーバとの認証に関する情報の無線通信による交換動作を一部省略できるようにしたことにより、認証に要する通信負担の軽減を実現できる。

#### 【図面の簡単な説明】

【図1】第1の実施形態に係る移動端末接続方法によるサーバ・クライアント間接続シーケンスを示す図である。

【図2】第1の実施形態に係る移動端末接続方法を適用するシステム構成を示す図である。

【図3】第1の実施形態に係る移動端末接続方法の実現に使用されるサーバの機能構成例を示す図である。

【図4】第1の実施形態に係る移動端末接続方法の実現に使用されるクライアントの機能構成例を示す図である。

【図5】第2の実施形態に係る移動端末接続方法を適用するシステム構成を示す図である。

【図6】第2の実施形態に係る移動端末接続方法の実現に使用されるサーバの機能構成例を示す図である。

【図7】第2の実施形態に係る移動端末接続方法の実現に使用されるクライアントの機能構成例を示す図である。

【図8】第2の実施形態に係る移動端末接続方法によるサーバ・クライアント間接続シーケンスを示す図である。

【図9】第3の実施形態に係る移動端末接続方法を適用するシステム構成を示す図である。

【図10】第3の実施形態に係る移動端末接続方法の実現に使用されるサーバの機能構成例を示す図である。

【図11】第3の実施形態に係る移動端末接続方法の実現に使用されるクライアントの機能構成例を示す図である。

【図12】第3の実施形態に係る移動端末接続方法によるサーバ・クライアント間接続シーケンスを示す図である。

【図13】第4の実施形態に係る移動端末接続方法を適用するシステム構成を示す図である。

【図14】第4の実施形態に係る移動端末接続方法の実現に使用されるサーバの機能構成例を示す図である。

【図15】第4の実施形態に係る移動端末接続方法の実現に使用されるクライアントの機能構成例を示す図である。

【図16】第4の実施形態に係る移動端末接続方法によるサーバ・クライアント間接続シーケンスを示す図である。

【図17】第5の実施形態に係る移動端末接続方法を適用するシステム構成を示す図である。

【図18】第5の実施形態に係る移動端末接続方法の実現に使用されるサーバの機能構成例を示す図である。

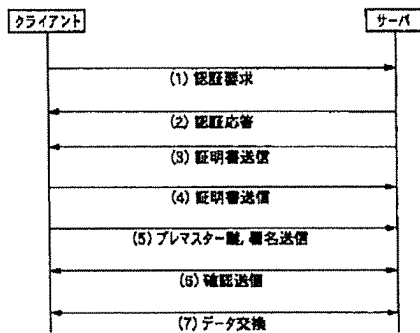
【図19】第5の実施形態に係る移動端末接続方法の実現に使用されるクライアントの機能構成例を示す図である。

【図20】第5の実施形態に係る移動端末接続方法によるサーバ・クライアント間接続シーケンスを示す図である。

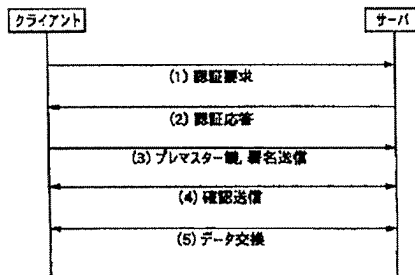
#### 【符号の説明】

1…サーバ、2…無線通信装置、3…クライアント、11、21…認証部、12、22…証明書格納部、13…一時的ID発行部、14、24…サービス実行部、15…通信部、16…証明書転送部、17…隣接サーバ情報格納部、18…経路上サーバ検索部、19…移動時間推定部、23…一時的ID格納部、25…無線通信部、26…直前サーバ位置情報格納部、27…移動経路入力部。

【図 1】

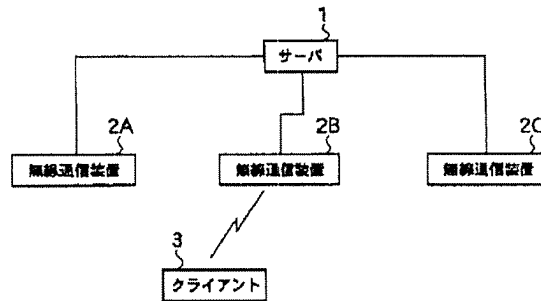


(a) 第1実施形態におけるサーバクライアント間初期シーケンス

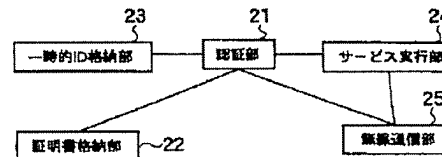


(b) 第1実施形態におけるサーバクライアント間再接続シーケンス

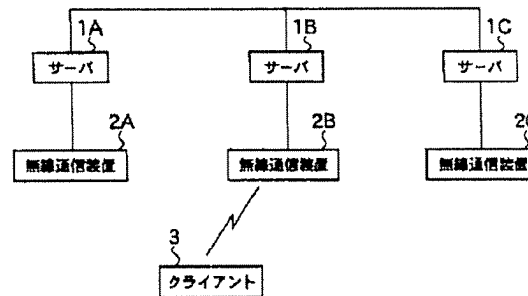
【図 2】



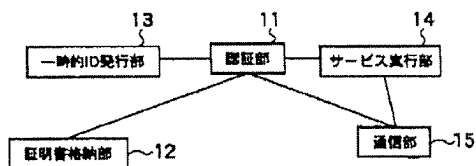
【図 4】



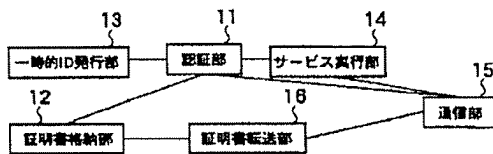
【図 5】



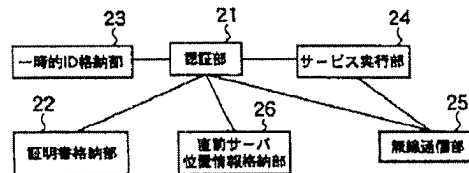
【図 3】



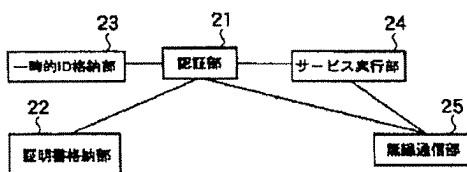
【図 6】



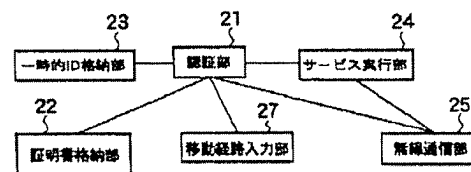
【図 7】



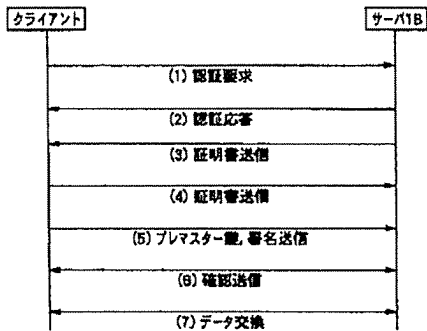
【図 11】



【図 15】

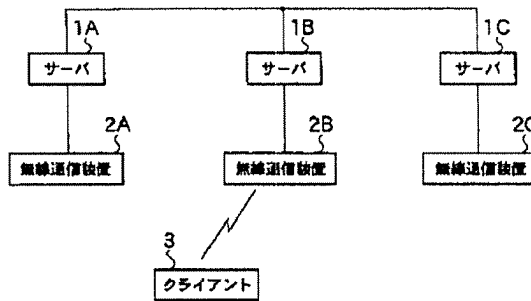


【図 8】

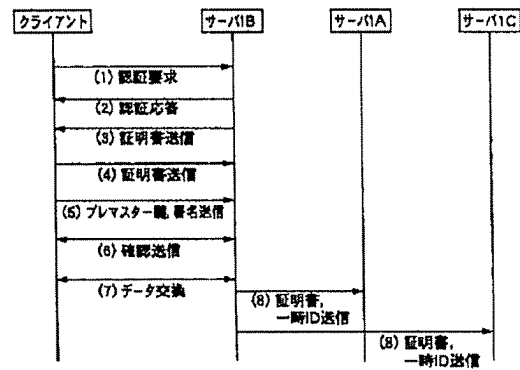


(a) 第2実施形態におけるサーバ/クライアント間初期シーケンス

【図 9】

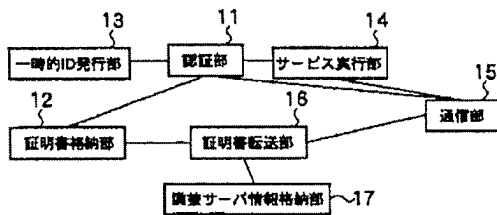


【図 12】

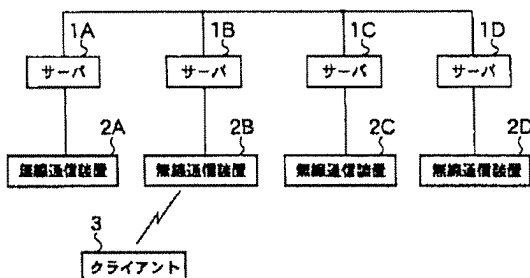


(a) 第3実施形態におけるサーバ/クライアント間初期シーケンス

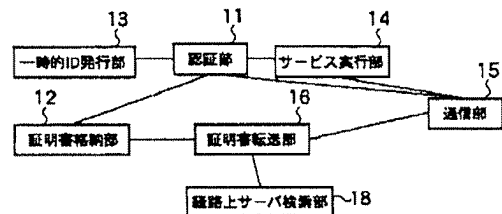
【図 10】



【図 13】

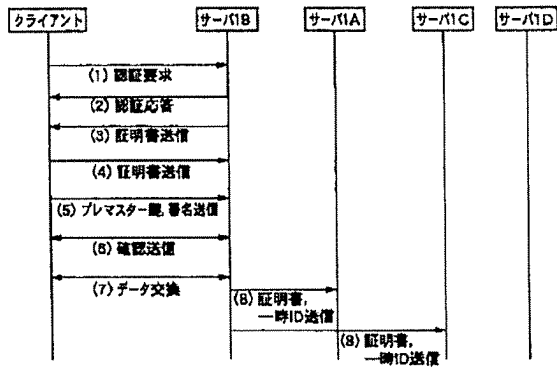


【図 14】



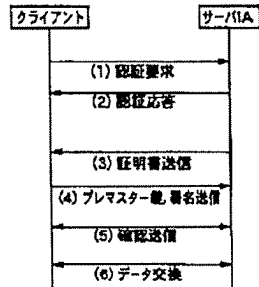
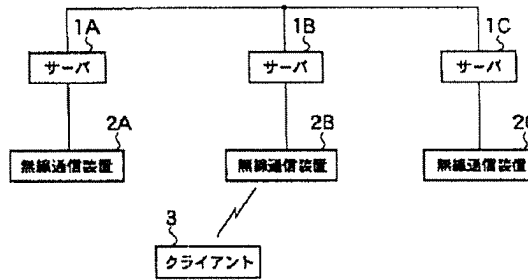


【図16】



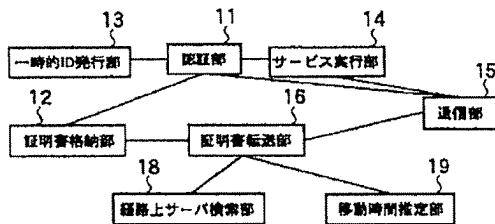
(a) 第4実施形態におけるサーバクライアント間初期シーケンス

【図17】

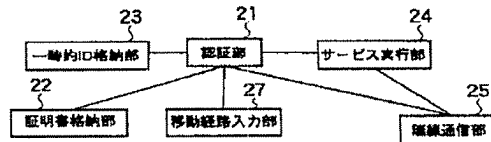


(b) 第4実施形態におけるサーバクライアント間再接続シーケンス

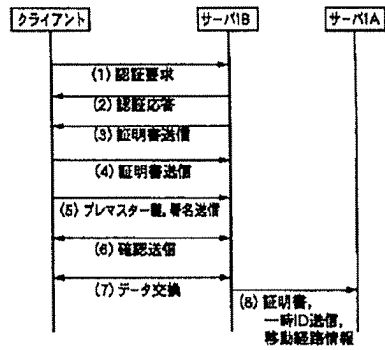
【図18】



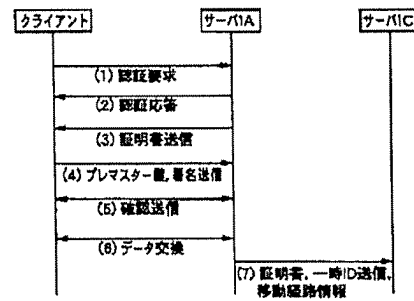
【図19】



【図20】



(a) 第5実施形態におけるサーバクライアント間初期シーケンス



(b) 第5実施形態におけるサーバクライアント間再接続シーケンス